



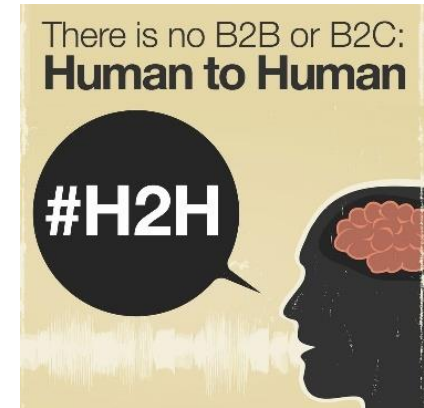
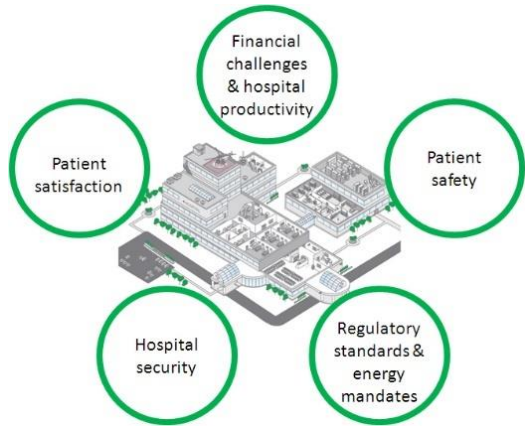
Evidence Based Security

Reality.. Or... Fantasy

Sumit Sehgal | Chief Healthcare Technical Strategist



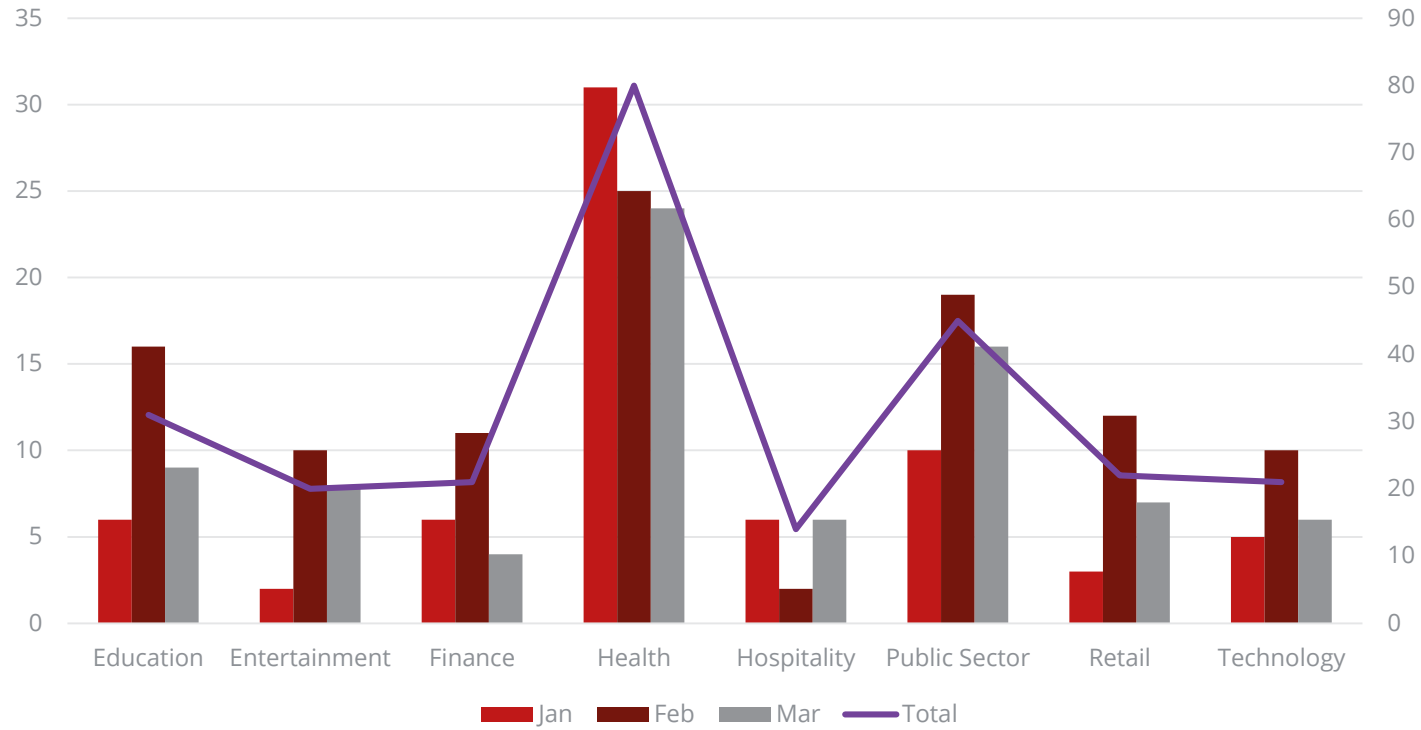
What makes healthcare information security different?



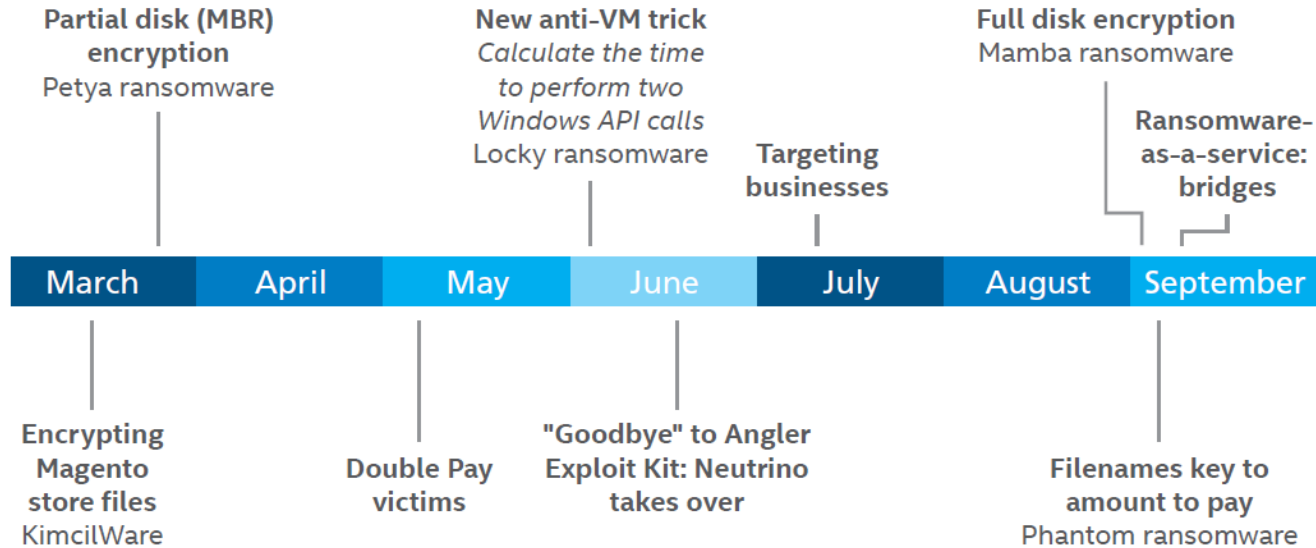
Goal is to achieve emotional and physical well being while managing complexity of large scale "always ON" environments.

What's coming after us?

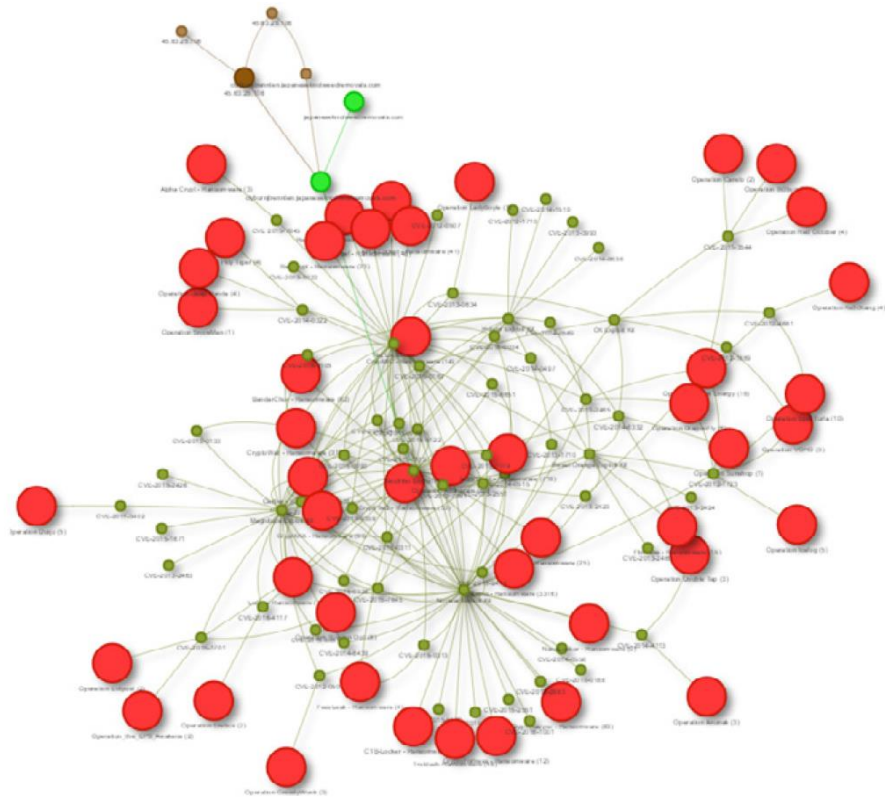
The threats are real...



And their evolution is as well..



Source: McAfee Labs.



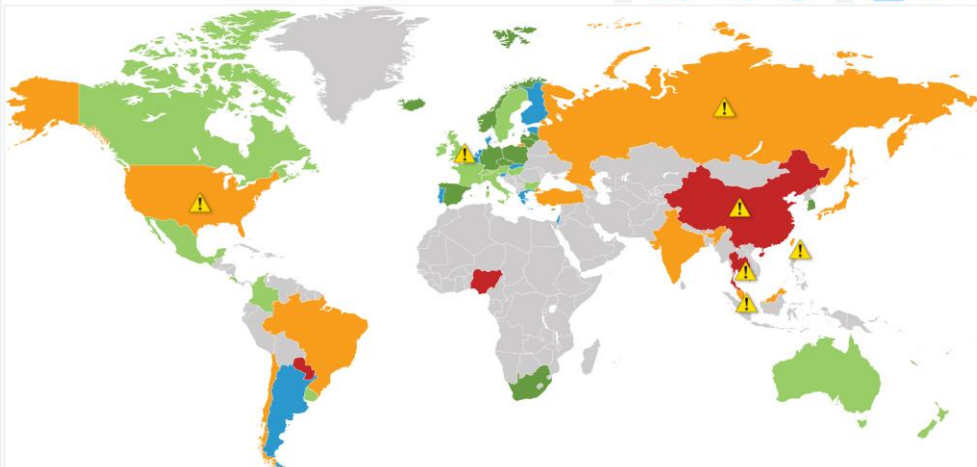
Source: McAfee Labs.

Data Telemetry is important especially if working internationally...

Global Heat Map

Country-specific regulations governing privacy and data protection vary greatly. Forrester's global heat map provides our clients with detailed, current information to help them successfully navigate each country's privacy regulations. **Preview the map by selecting the US or UK information below.**

View by: ▼



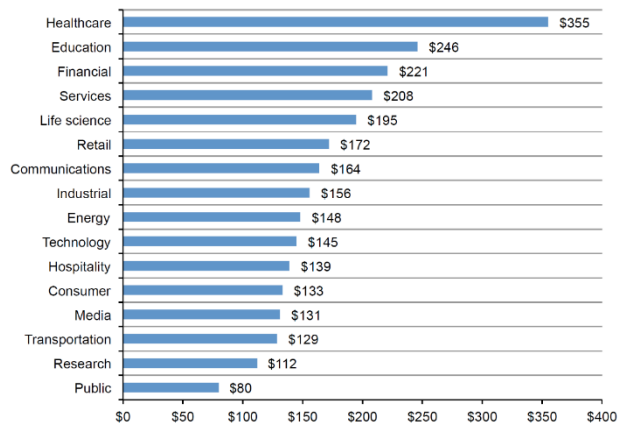
■ Most restricted ■ Restricted ■ Some restrictions ■ Minimal restrictions ■ Effectively no restrictions
■ No legislation or no information ■ Premium content ▲ Government surveillance may impact privacy

Source: Forrester's Global Data Protection and Privacy Heatmap

Its just not about the value of data... it's also about how you affect it.....

Figure 4. Per capita cost by industry classification

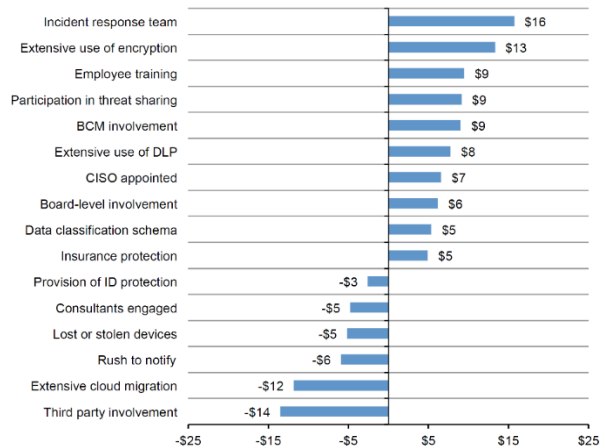
Consolidated view (n=383), measured in US\$



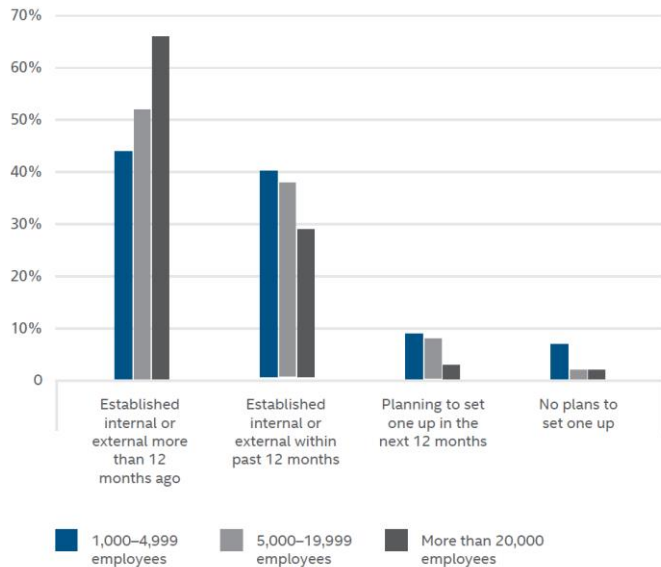
Can you guess
what is worth
~**\$1100/Record?**

Figure 8. Impact of 16 factors on the per capita cost of data breach

Consolidated view (n=383), measured in US\$

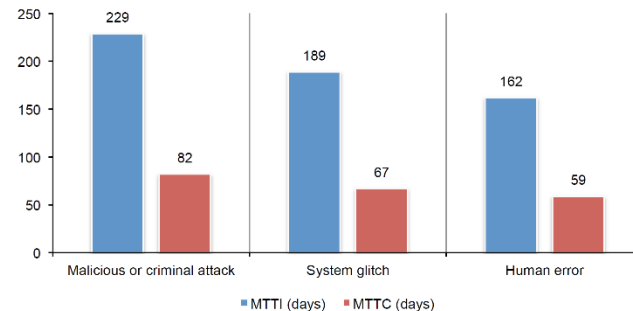


So if everyone is looking at threats....



Why is the response downright... depressing??

Figure 21. Mean time to identify and contain data breach incidents by root cause (in days)
Consolidated view (n = 383)



To maximize our focus...We need to improve threat defense efficacy

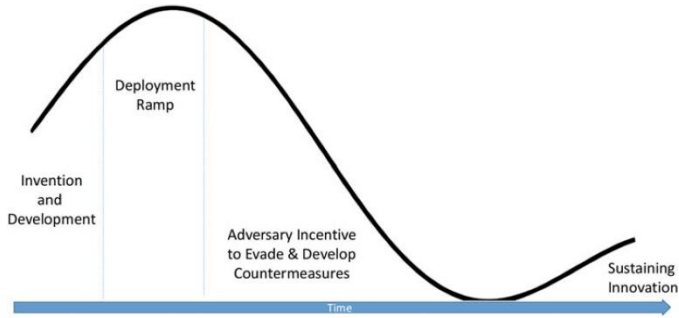


Figure 8-1. Grobman's Curve of Threat Defense Effectiveness

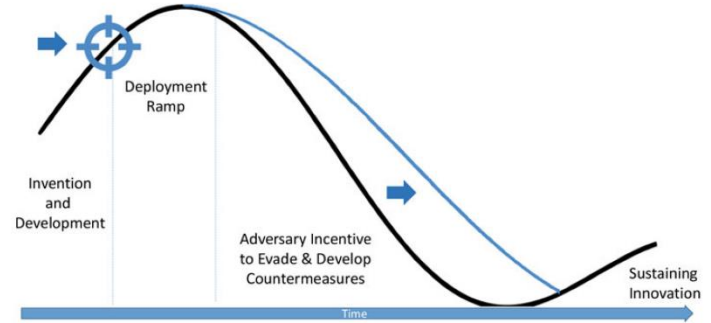
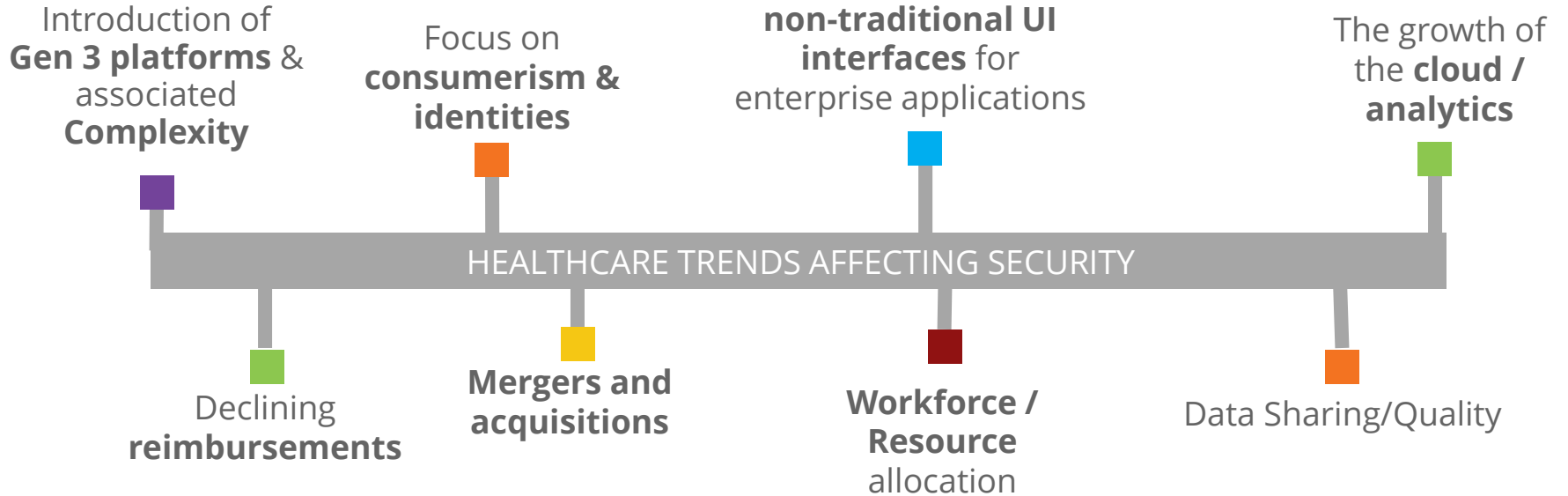


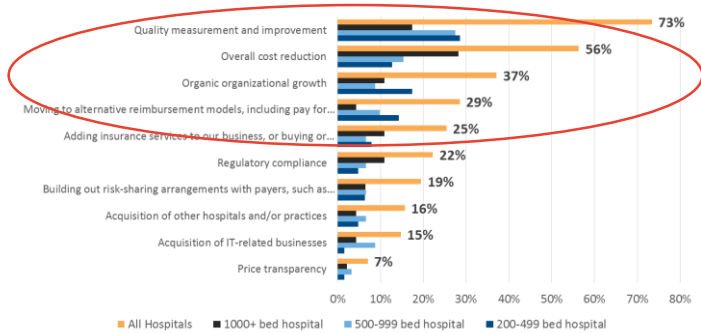
Figure 8-2. Grobman's Curve of Maximizing Defense Effectiveness

Investment with /
without purpose..

Insight #1: Flux in the industry

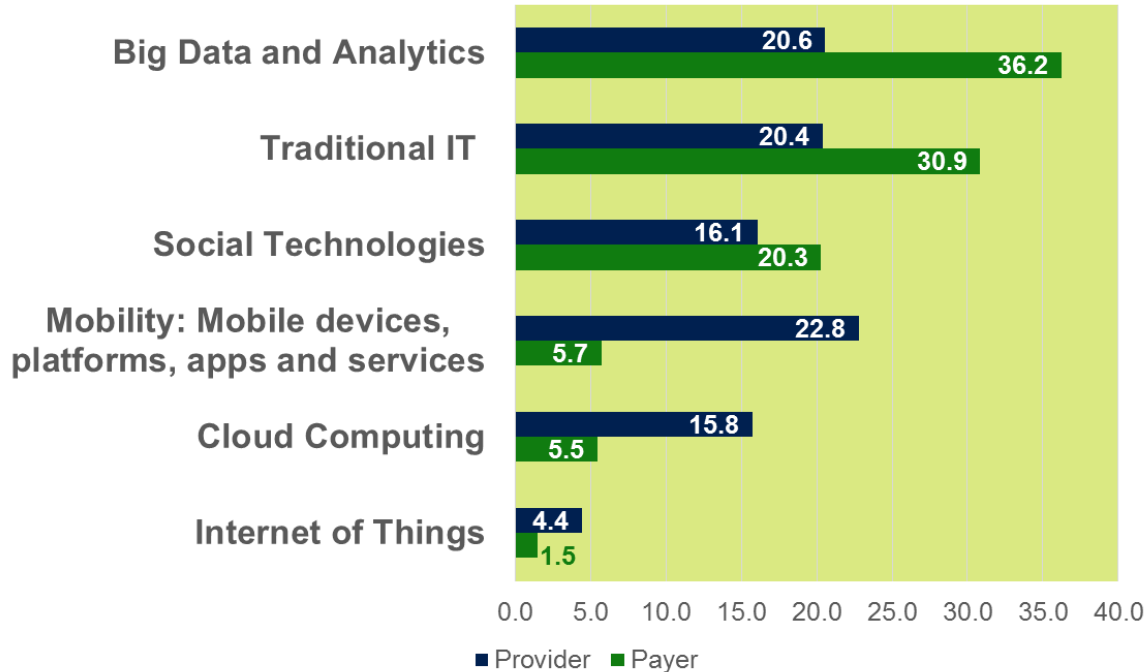


Insight #2: Disconnect with Org Strategy & Cost allocation



Source: Healthcare Provider Technology Spend Survey, IDC, October, 2015

Insight #3: Priorities for Payers and Providers

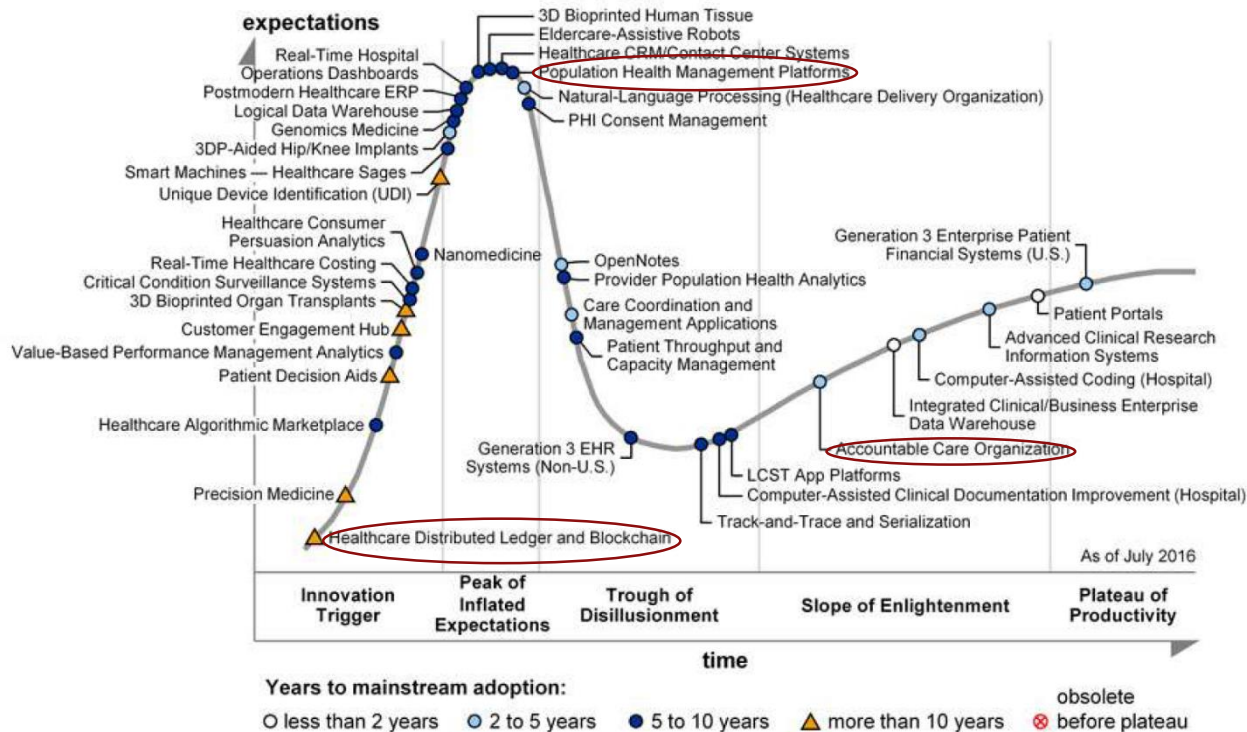


- **36%** of **payers** report **Big Data and Analytics** as #1 priority
- **23%** of **providers** report **Mobility** as #1 priority

Source: IDC Health Insights Payer Survey, June 2015, 2015-2016
Healthcare Provider Technology Spend Survey, IDC, October, 2015

Insight #4: It will take time for next gen models to be effective

Figure 1. Hype Cycle for Healthcare Providers, 2016

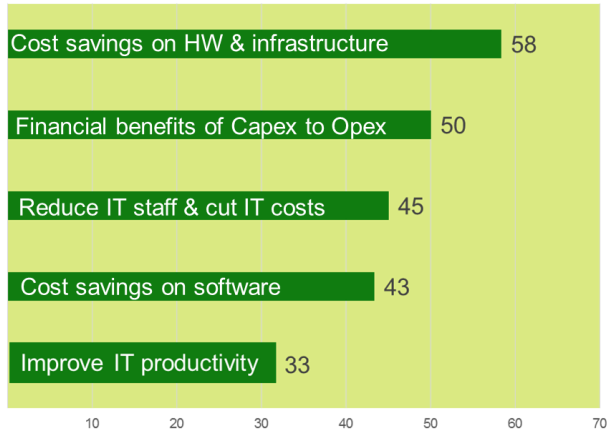


Source: Gartner (July 2016)

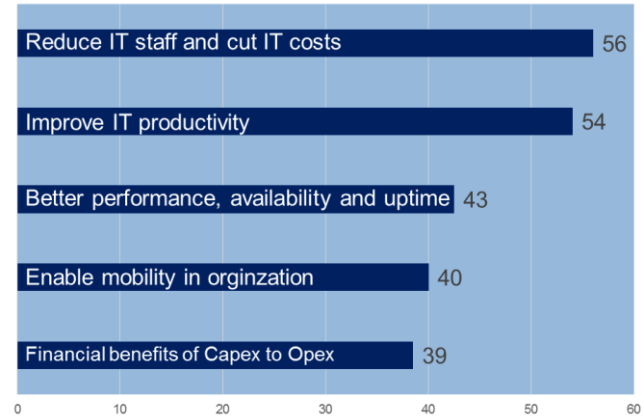
Insight #5: Cloud will power a lot of this stuff...

Yet the genesis of the cloud varies in the industry..

Payers Focused on Cost



Providers... on Productivity



Insight #6: IoT in healthcare is also about the people...



**Telemedicine /
Telehealth**

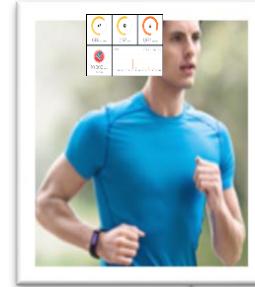
IOT



**Remote Health
Monitoring**



**Connected
Health**



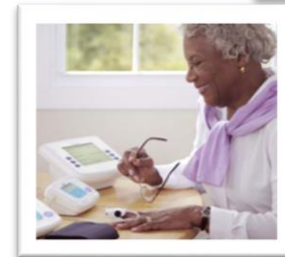
Fitness



In utero



Babies



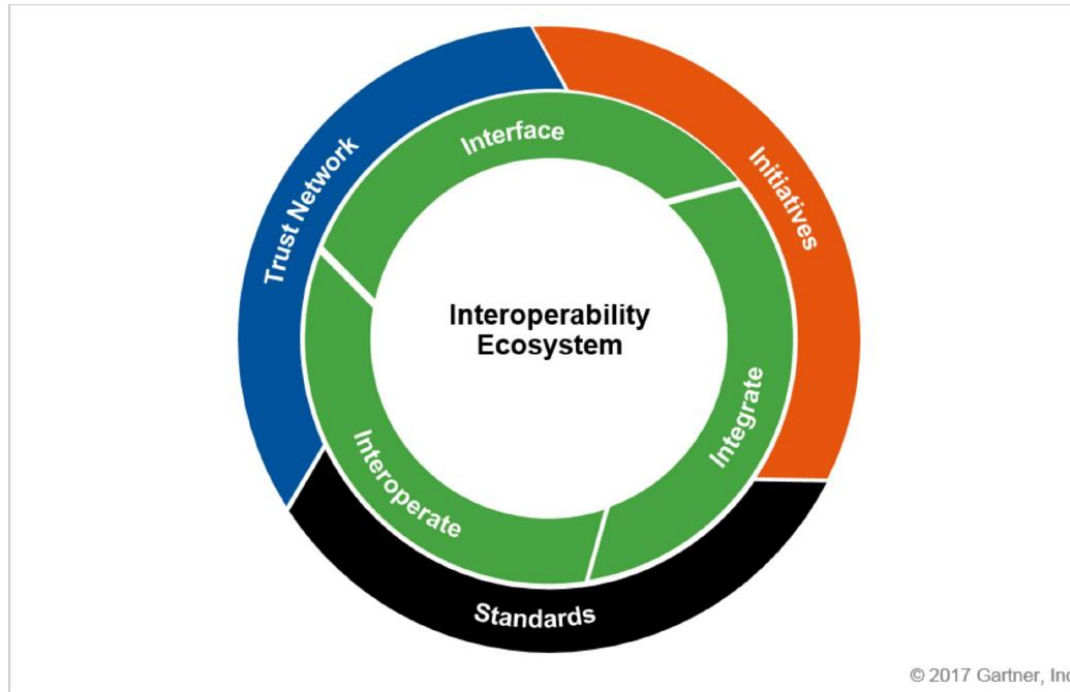
Seniors



Children

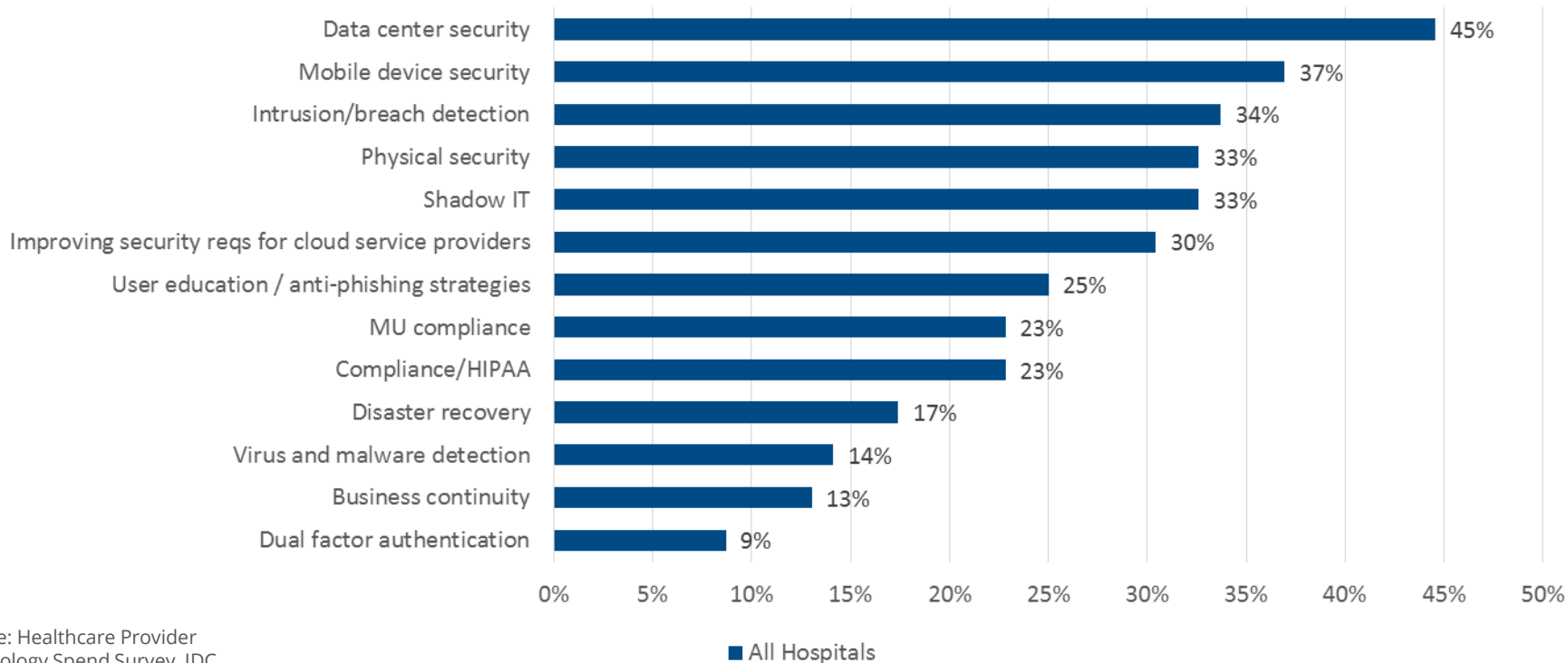
Source: IDC Health Insights' Connected Health and Value-based IT Initiatives Survey, June 2016

Insight #7: Interoperability can help.. Lets see how..



Source: Gartner (February 2017)

Insight #8: Issues of muscle memory when allocating security budgets



Source: Healthcare Provider
Technology Spend Survey, IDC,
October, 2015

Wrong Mission X Outdated Approach = Failure

Normally the healthcare CISO is focused on

1. Operational Efficiency
2. Regulatory Compliance
3. Data Context
4. Risk Mapping
5. Architecture Agility AT SCALE...

But the problem really is dealing with an inadequate threat model...

		Patient Health		Patient Records	
Adversary	Targeted (Specific Victims)	Untargeted (Indiscriminate)	Targeted (Specific Victims)	Untargeted (Indiscriminate)	
Individual / Small Group				YES	
Political Groups / Hacktivists /			YES		
Organized Crime	YES		YES	YES	
Terrorism / Terrorist Org.	YES	YES			
Nation States	YES	YES	YES	YES	

With missing asset alignment..

Patient Assets	Hospital Assets
Patient health	Research / IP
Patient records	Business advantage
Service availability	Hospital finances
Community confidence	Hospital reputation
	Physician reputation

Source: Securing Hospitals by ISE

In addition to a complex attack surface

Data flows are critical

Focus on data protection is NOT sustainable

Need to account for middleware in addition to application and infrastructure security

Align ERM with QI and Clinical Risk



Source :Securing Hospitals by ISE

Regulation of Choice...

- HIPAA / HITECH
 - Pay attention to updates and guidelines issued by HHS, ONC, FDA and OCR in the last 18 months
- State Security / Privacy regulations
- FTC Red Flag Rules
- PCI – DSS Implications
- FISMA Implications for clinical research
- The Joint Commission requirements for information management
 - Grossly underestimated from organizational importance to security strategy

Leads to fun conversations when talking about the buzz word...
"Context"...

For Health IT ... that is focused on 3 areas.... But does order matter?

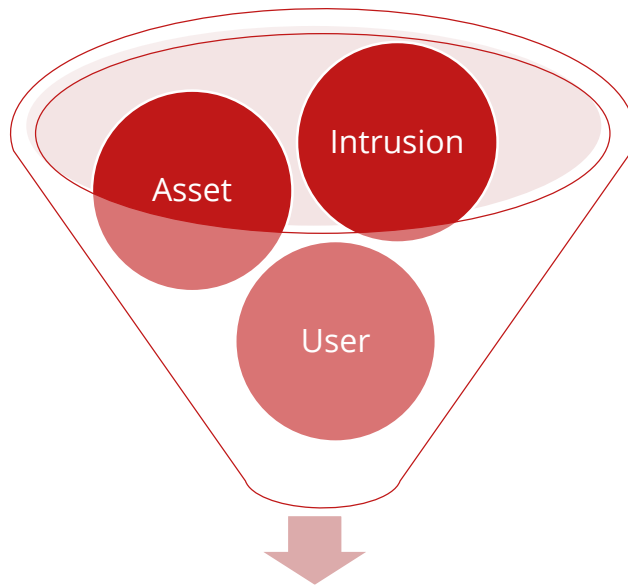
These 2 matter most for treating patients



Enough about failure... lets talk evidence based outcomes...

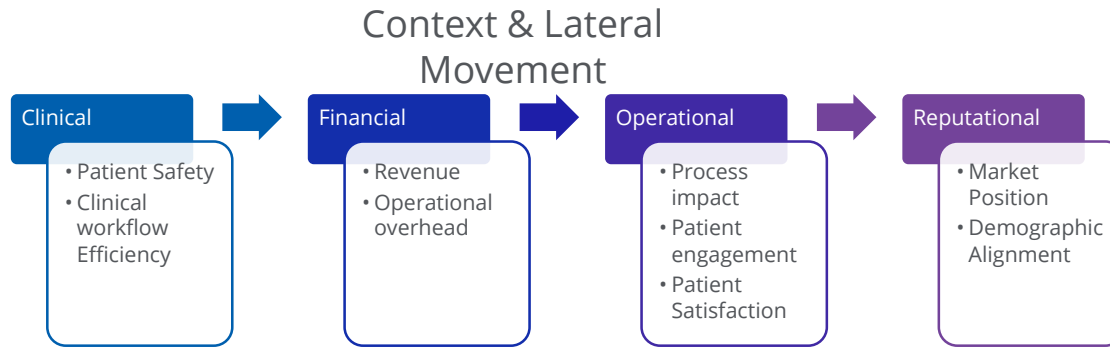


<https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp>

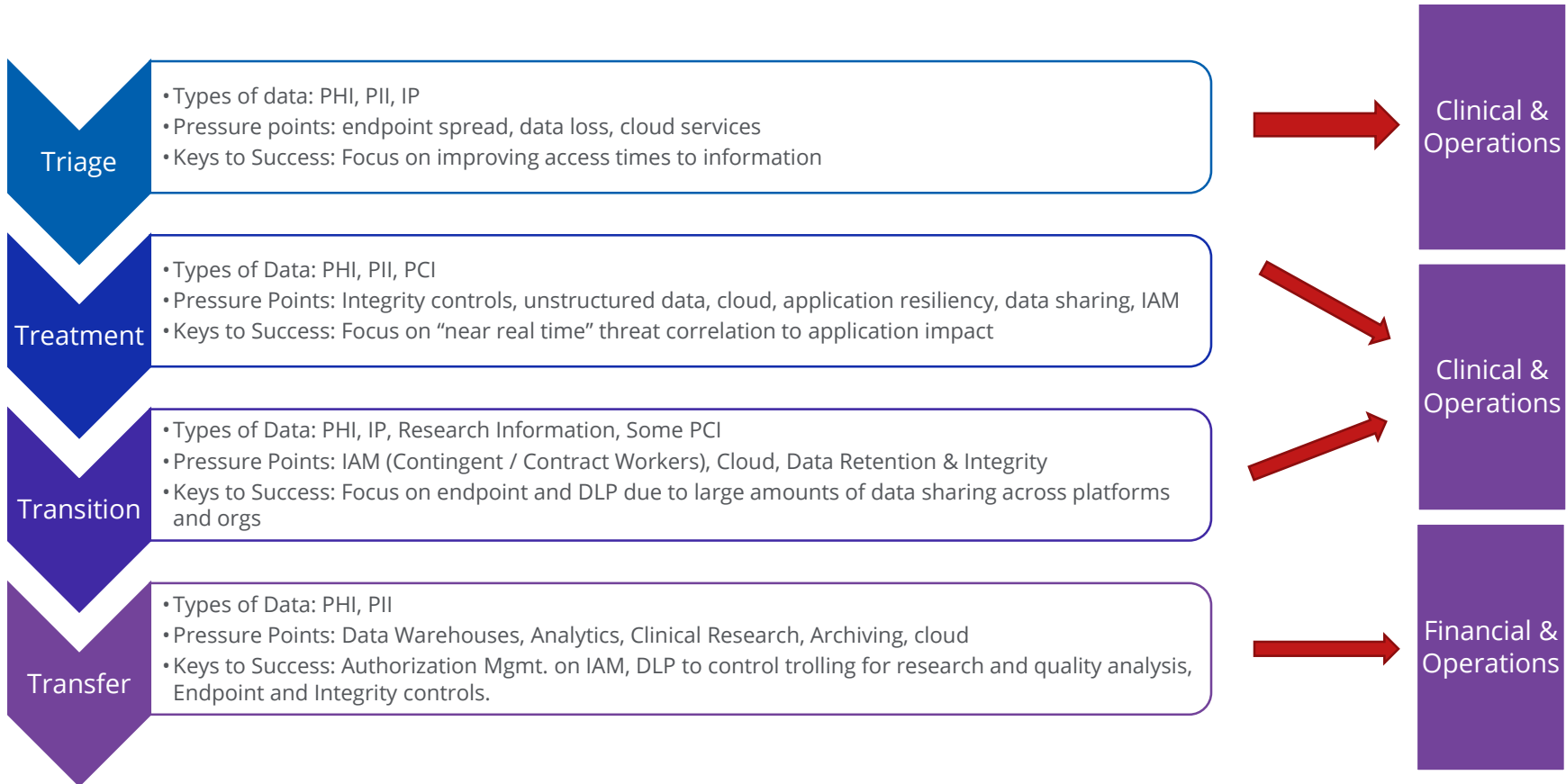


Taking information from security solutions to add context with the goal to color risk thresholds....

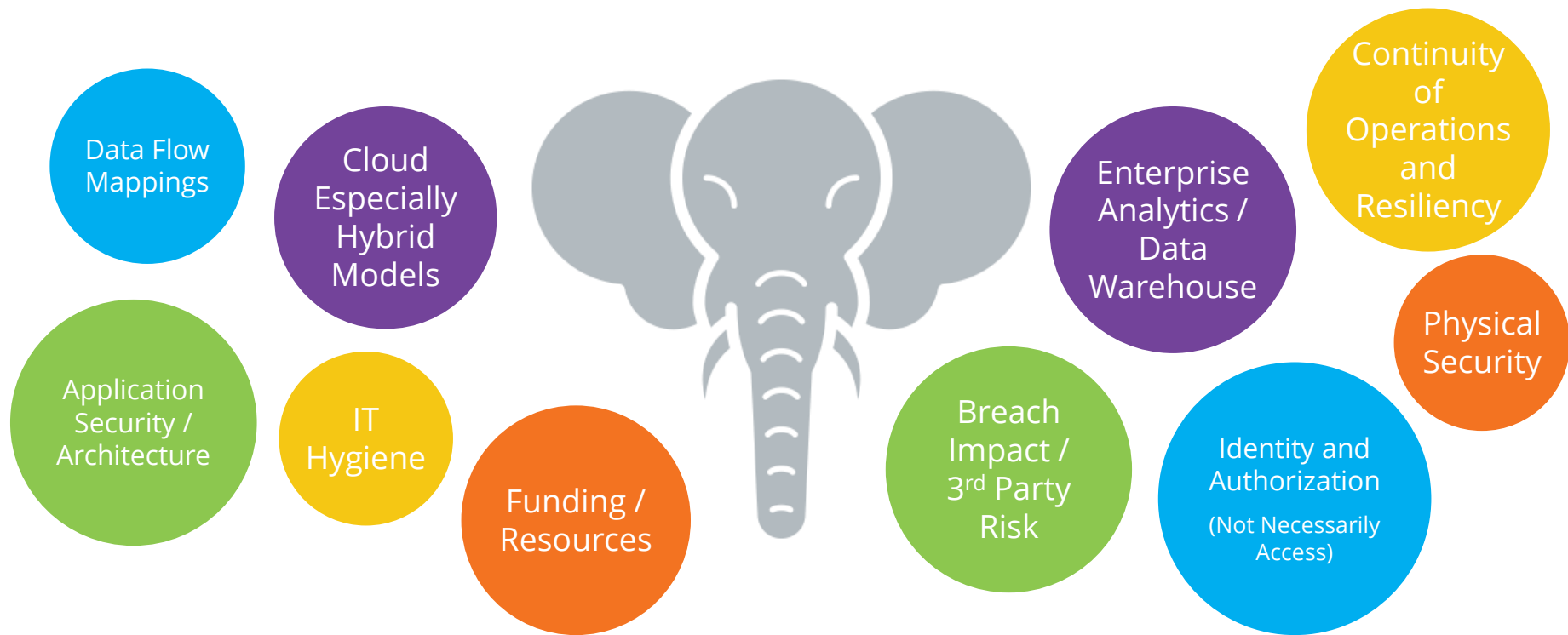
CISO Nirvana...



Example of Data flow analysis

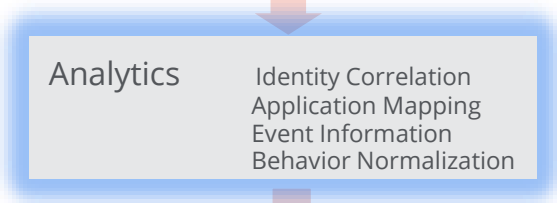
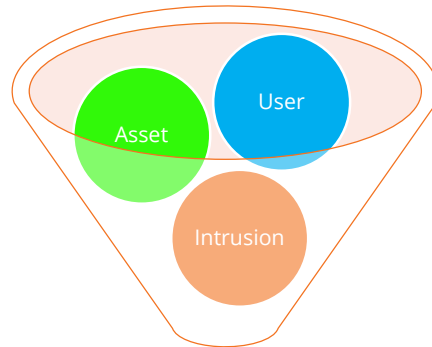


Before the solution output can be “useful”...
We have to talk about the IT elephants' in the room:



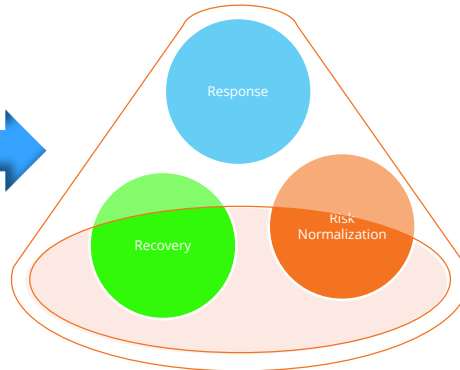
Improving Signal to noise

Everyone is doing this

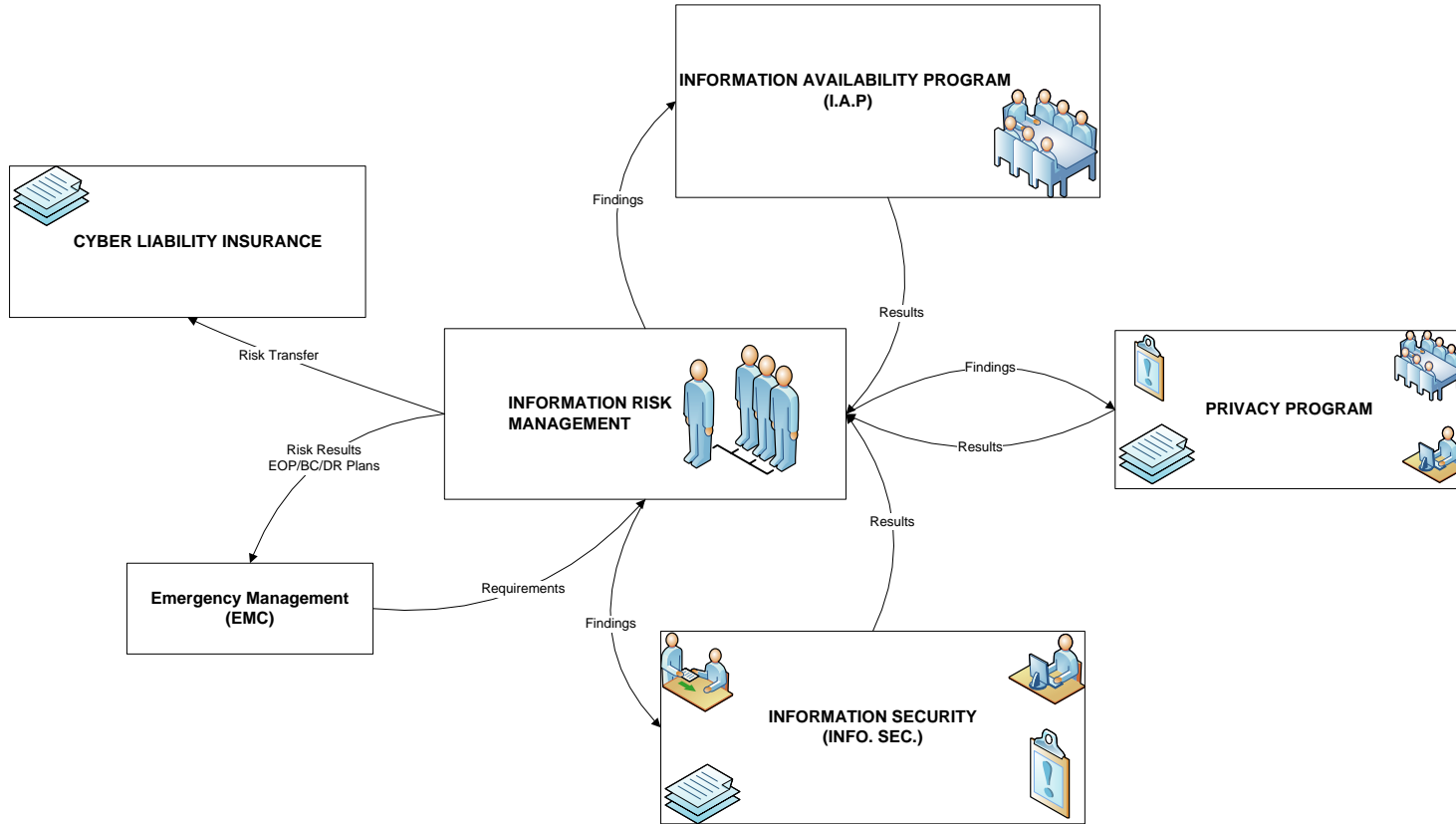


Focus on producing
"Technically Correct"
AND "Useful"
information

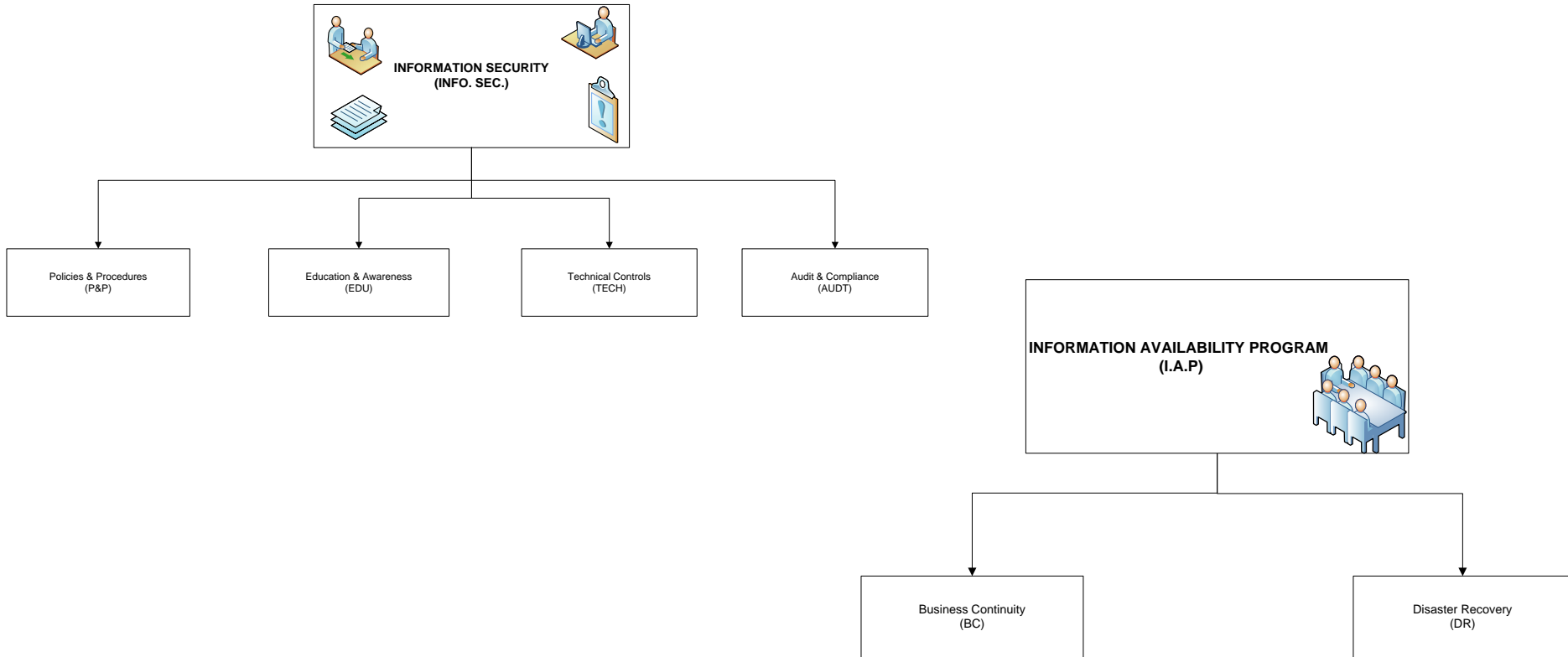
This is where you see
benefits of
operational
"efficiency" and cost
reduction outside of
security



First Step



Second Step



Once the paper stuff is done.. In what order do I address stuff



Fact Check: When Security Starts to Work Together

Average timeline of tangible improvements to security posture is **2 - 3 years**

Info Sec Operating Budget grows **~1% to ~5%**

Average financial savings from consolidation is **~10 - 30 %** over 2 years

Average analyst time spent on incident investigations reduces from *3 - 72 hours* to **15 - 60 min**

Security FTE Stats

- Per 1000 end users
 - Before: 0.4 - 0.5 FTE
 - After: 2 - 3 FTE



McAfee, the McAfee logo are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries.
Other names and brands may be claimed as the property of others.
Copyright © 2017 McAfee LLC.